Description

Method for transmitting encrypted user data objects

The present invention relates to a method for handling, in particular transmitting, encrypted user data objects which are provided by a data provisioning component and transmitted to a telecommunications device such as, for example, a mobile phone. The present invention relates in particular to a method which enables a user of the telecommunications device to download different rights or rights objects from the data provisioning component to the telecommunications device in return for an appropriate charge.

A method or, as the case may be, a service for reliable and accountable downloading of user data objects to a telecommunications device, in particular in the embodiment of a mobile radio device or mobile phone, in a data communications network is currently under discussion. In a proposed scheme the downloading of the user data objects to the mobile radio device is intended to be implemented by means of a protocol specified by the WAP Forum (WAP: Wireless Application Protocol) or an Internet protocol (e.g. Hypertext Transfer Protocol: HTTP). The downloading service is specified here in such a way that a user with an application program which is available on the mobile radio device and which is referred to as a download client is to be allowed to download any user data objects which are provided by one or more data provisioning components, in particular servers or, as the case may be, download servers of service providers or content providers in the data communications network. A possible embodiment of the

service makes provision for a downloadable user data object to be provided with restrictions in relation to its usage by the user of the mobile radio device. This can be used for example to restrict the number of uses of the user data object or also the usage period. The practical implementation is effected by the description of the restrictions using a suitable language such as, for example, ODRL (Open Digital Rights Expression Language), whereby the download client or another special application, called a DRM agent, receives the rights description for management of the rights associated with a (digital) user data object (DRM: Digital Rights Management), evaluates it, stores it in a protected memory area that is not accessible to the user on the mobile radio device, and, in response to a request by the user to use the object, grants or does not grant said rights in accordance with the rights description. The user data object itself can be protected against unauthorized access either by being stored in encrypted form in a freely accessible memory area on the mobile radio device or by being managed by a special application, for example the DRM agent, which does not allow any unauthorized access to the object by the user.

According to a variant specified by the WAP Forum for the management of DRM-protected contents, a user data object provided by a data provisioning component is encrypted and finally is packed for transport and for storage onto a telecommunications device such as a mobile radio device in a so-called container file or a so-called container object (which, for example, has been assigned the data type or content type "Application/VND.OMA.DRM.Content"). By means of a service for reliable downloading of content by a data provisioning component (content download) the encrypted

user data object is packed in the container object and transmitted to the telecommunications device using WAP protocols (such as, for example, the WSP: Wireless Session Protocol) or Internet protocols (such as, for example, the HTTP). A so-called rights object is transmitted to the telecommunications device separately from the encrypted user data object, for example by means of a WAP push. The rights object contains a description of the rights granted to the user for using the encrypted user data objects, a reference to the container object which enables the rights object to be assigned to the corresponding container object, and a key by means of which the encrypted user data object can be decrypted so that it can subsequently be used. A special device or application, which may be the above-mentioned DRM agent, is necessary on the telecommunications device, such as the mobile radio device, in order to use the combination of the encrypted user data object packed in the container object and the rights object. After the transmission of the rights object to the telecommunications device the rights object is transferred directly to the DRM agent which is responsible for the management and safekeeping of the secret, namely the key for decrypting the encrypted user data object. In practice the DRM agent stores the rights object on the telecommunications device and protects it against unauthorized access by other applications or users. The first step when an encrypted user data object is to be used is that the DRM agent is activated.

The latter searches for a rights object that matches the container object in the memory area managed by it in the telecommunications device on the basis of the identification contained in the container object and also in the rights object, checks whether rights can be granted

for the requested usage type (such as, for example, "playing back" music data or "displaying" image data, etc.) and decrypts the user data object using the key from the rights object if the rights can be granted. By means of the above described method, wherein an encrypted user data object and a rights object separate therefrom can be used, the value of digital data is no longer represented by the (encrypted) user data object or the container object itself, but rather by the rights object and the key contained therein, without which, of course, the encrypted user data object cannot be used. Thus, in this case the encrypted user data objects can be stored in packed form in the container objects on the telecommunications device and be freely accessible. This also allows encrypted user data objects, packed in container objects, to be forwarded by a user to one or more other users, a process referred to as "superdistribution".

In order to make the encrypted user data object contained in a forwarded container object usable, an individual user must download a suitable rights object from a rights provider that may be identical to the content provider providing a specific user data object.

The method just described, in which in order to make user data objects usable it is necessary firstly to download a container object containing an encrypted user data object, and secondly to download a rights object from an identical or from different data provisioning component(s), does, however, have the disadvantage that before downloading a rights object a user has no means of checking whether the rights object offered for example by an arbitrary provider does in fact enable the use of the encrypted user data object which is already present, stored in the container

object, on the user's own telecommunications device, i.e. whether the offered rights object comprises for example the right key for decrypting the encrypted user data object contained in the container object. A further disadvantage is that a user without a purchased or downloaded rights object has no means whatsoever of checking whether the encrypted user data object received by his or her telecommunications device or even the entire container object is undamaged.

It is therefore the object of the present invention to create a means by which a user is rendered capable of checking the integrity or, as the case may be, usability of an encrypted user data object stored on his or her telecommunications device.

This object is achieved by the subject matter of the independent claims. Advantageous embodiments are the subject matter of the dependent claims.

With a method for handling and/or transmitting encrypted user data objects, wherein a data provisioning component provides user data objects, a user data object of said kind is first encrypted in order to protect it against an unauthorized access. Next, a checksum of the encrypted user data object (or of the entire container object) is determined. This can be calculated for example by means of a conventional hash algorithm. A container file or container object which has a content section and a description section is also generated. The encrypted user data object is provided in the content section of the container object, while the checksum just determined is provided in the description section. The container object

thus contains two data areas which are accommodated independently of each other, yet which are related in terms of their content (encrypted user data object associated with the checksum determined by said object) and which therefore permit an integrity check in a comparison of this data. Finally the generated container object is transmitted to a first telecommunications device of a first user.

It should be noted here that it is possible that the still unencrypted user data objects are provided by a first data provisioning component, while they are encrypted by a second data provisioning component connected to the first data provisioning component and are packed together with a checksum determined in this regard into a container object and finally offered to a user for downloading to his or her telecommunications device. In a case such as this, rather than referring to one or more individual data provisioning components it is also possible to speak of a data provisioning system which comprises the individual data provisioning components for providing user data objects or, as the case may be, for encrypting, packing and providing user data objects. In addition to the possibility that a container object is transmitted directly by a data provisioning component or, as the case may be, a data provisioning system to a telecommunications device assigned to a user, it is also possible that the container object reaches the first user or the latter's telecommunications device via one or more second or further telecommunications devices of other users.

A container object generated for example according to the above method in a data provisioning component is advantageously analyzed after its reception by the first

telecommunications device in such a way that the checksum provided in the container object is first extracted from the description section of the container object. Next, the checksum is determined a second time from the encrypted user data object provided in the content section of the container object. The checksum just determined a second time is then compared with the extracted checksum so that, in the event that the two checksums tally, it can be concluded that the encrypted user data object has been transmitted correctly or, as the case may be, that the user data object is undamaged. This type of analysis of a received container object can be performed by a special application of the (first) telecommunications device which is specially designed for managing usage rights for digital data or data objects, i.e. a so-called DRM agent (DRM: Digital Rights Management). Such a comparison of the extracted and newly determined checksums thus enables it to be confirmed whether, in particular in the case of a superdistribution of container objects, an encrypted user data object has been incompletely transmitted or whether a user data object has been for example selectively tampered with.

It should be noted that it is possible that not just one encrypted user data object may be provided in a container object or, as the case may be, in its content section, but also a plurality thereof. Accordingly a checksum must be determined in each case for this plurality of encrypted user data objects, with the respective checksums having to be provided in the description section of the container object.

In an integrity check, finally, the respective checksum of each encrypted user data object to be analyzed can then be

determined and compared with the respective checksum provided in the description section. In this way it is possible to combine for example a plurality of related user data objects (linked for example on the basis of their related subject matter, such as images of the same object at different resolutions) in a single container object and transmit said container object.

In order to be able to use an encrypted user data object which is packed in a container object and has been provided or received on a telecommunications device it is also necessary to provide a rights object which firstly has assignment information for assigning the rights object to an encrypted user data object or to a container object which contains the encrypted user data object. The rights object must also contain decryption information for decrypting the encrypted user data object in order to make the user data object usable for the user, i.e. to permit a music file to be played back for example. The rights object can further comprise rights information for describing the usage rights of the encrypted user data objects. In this case the usage rights can include, for example, how long the use of a user data object is permitted, how often said use is permitted, or, for example in the case of a multimedia user data object, the use of which medium is permitted during said use (in the case of a video clip with musical accompaniment, for example, whether just the music may be listened to or whether the associated video clip may also be viewed). The rights object can be generated for example by a data provisioning component which also provides or generates the container object, but it can also be generated by a different data provisioning component

which is in turn part, for example, of a higher-level data provisioning system.

Since, as already mentioned, the value of an encrypted user data object depends on the assigned rights object which grants the user the usage rights for the user data object, a provider of rights objects (which may also be identical with the provider of user data objects) will charge a user for a rights object immediately after transmitting the said rights object to the user or the latter's telecommunications device. This means that the user, who can choose for example from a plurality of rights objects, would therefore have no means of checking whether the chosen rights object matches the encrypted user data object stored on his or her telecommunications device before he or she downloads the rights object and has to pay for it. Thus, in order to enable a user to check, prior to the transmission or downloading of a specific rights object, whether the rights object actually permits the use of the encrypted user data object present in the container object on his or her telecommunications device, i.e. whether the specific rights object will contain the right key for decrypting the encrypted user data object, according to an advantageous embodiment a verification object or confirmation object assigned to the rights object is generated which has assignment information for assigning the rights object to an encrypted user data object and a checksum of the encrypted user data object. This means that a confirmation object is generated in the data provisioning system, in particular by the data provisioning component which also provides the rights object, which confirmation object does not enable a decryption of an encrypted user data object, but permits a compatibility check to determine

whether a rights object assigned to the confirmation object matches or is compatible with a user data object that is present on the user's telecommunications device.

In this regard, according to a further advantageous embodiment of the invention a request is submitted on the part of the first telecommunications device to the data provisioning system of a content provider or a data provisioning component of said system to the effect that the confirmation object assigned to a specific rights object is transmitted to the (first) telecommunications device. The confirmation object is then transmitted by the data provisioning component or, as the case may be, the data provisioning system to the first telecommunications device, where finally the checksum is extracted from the confirmation object. A comparison can now be made between the checksum extracted from the confirmation object and the newly determined checksum or the checksum provided in the description information of the container object in order to be able to conclude, in the event that the checksums tally, that the rights object assigned to the confirmation object and the encrypted user data object transmitted in the container object to the first telecommunications device are compatible. This means that it is now possible, without having to transmit the actual rights object, to check by means of the confirmation object assigned to the rights object or by means of the checksum provided therein whether the rights object is compatible with the user data object provided from the telecommunications device. It is possible here that the integrity check on the encrypted user data object contained in the container object can be performed before the request for the confirmation object, during the request or after the request for the confirmation object.

However, the integrity check is advantageously performed after reception of a container object and prior to a request for a confirmation object or rights object in order not to have to make the request for confirmation or rights objects unnecessarily in the event of a defective or erroneous encrypted user data object or container object.

If the check on the confirmation object with regard to the encrypted user data object present in the container object is completed with a positive result, the (first) telecommunications device can send the positive check result in the form of a status report to the data provisioning component providing the confirmation object or, as the case may be, the rights object assigned thereto. The data provisioning component can thereupon independently transmit the associated rights object to the first telecommunications device. It is, however, also possible that the first telecommunications device does not immediately send off a status report concerning the successful check on the confirmation object, but sends a request message at a later, self-determined time to the data provisioning component providing the rights object assigned to the confirmation object so that finally said data provisioning component transmits the rights object to the first telecommunications device. It is, however, also possible that the first telecommunications device directly requests a specific rights object from a data provisioning component providing said rights object by means of a request message provided for the purpose, only after an integrity check on a received container object.

According to a further aspect, in a method for handling or, as the case may be, making usable encrypted user data

objects, an encrypted user data object is provided in a first telecommunications device, for example in that it has been transmitted by a data provisioning component or a further telecommunications device and has possibly been checked for integrity according to an above method. The telecommunications device then requests description information relating to the content of the encrypted user data object from a data provisioning component. The requested description information is then transmitted to the first telecommunications device by the data provisioning component. A check is now made in the telecommunications device to verify whether the content with attributes specified in the description information can be used by the first telecommunications device. If the check on the attributes specified in the description information is successful, a confirmation object is requested from the data provisioning component, which confirmation object is assigned to a rights object (RO) assigned to the encrypted user data object in order to check the compatibility of the rights object and the encrypted user data object. Through the request for the description information it is now possible that the telecommunications device first checks whether the stored user data object is usable at all (if, for example, the telecommunications device has no means of outputting audio or music, a user data object having a music content would not be usable on the telecommunications device).

Advantageously the rights object is transmitted by the data provisioning component to the first telecommunications device upon successful checking of the compatibility of the rights object and the encrypted user data object.

The encrypted user data object can be provided in a content section of a container object. The container object can also have a description section in which a checksum of the encrypted user data object is provided. Moreover, the address of the data provisioning component for requesting the description information and/or the confirmation object can also be provided in the description section of the container object.

Advantageously the confirmation object has a checksum of the encrypted user data object, whereby the check on the compatibility of the rights object and the encrypted user data object is performed by means of the following steps. The checksum is extracted from the confirmation object. Next, the checksum extracted from the confirmation object is compared with the checksum provided in the description section of the container object in order to be able to conclude, in the event that the two checksums tally, that the rights object assigned to the confirmation object and the encrypted user data object provided in the container object on the first telecommunications device are compatible.

As mentioned already, it is possible that, in the event of a successful compatibility check of the confirmation object assigned to the rights object and the encrypted user data object transmitted in the container object on the first telecommunications device, a first confirmation message can be transmitted from the first telecommunications device to the data provisioning component providing the rights or confirmation object. It is furthermore possible that, providing in particular no check of the rights object is performed using a confirmation object, a second

confirmation message is sent by the first telecommunications device to the data provisioning component when the first telecommunications device has received the rights object from the data provisioning component. According to a further advantageous embodiment the user of the first telecommunications device is then charged on the basis of the reception of the first and/or second confirmation message from the data provisioning component for the transmitted rights object or, as the case may be, the user is sent charging information so that he or she can pay for the received rights object.

According to an advantageous embodiment the first and/or the further telecommunications devices and the data provisioning system including the data provisioning components provided therein (for container objects, confirmation objects or rights objects) are part of a telecommunications network. It is possible in this case that the first and the further telecommunications devices are in each case part of a telecommunications network, whereby the individual telecommunications devices do not have to be part of the same telecommunications network. Accordingly a data provisioning component of the data provisioning system, which component is embodied in particular as a data server of a service provider or content provider, can be provided in a telecommunications network which is connected to the telecommunications network or networks which are assigned to the first and the further telecommunications devices.

In order to be able to use the method for transmitting user data objects as flexibly as possible, the first and/or the further telecommunications devices can preferably be

embodied as a mobile telecommunications device and at the same time comprise in particular a radio module or mobile radio module.

In this case the telecommunications device can be embodied for example as a mobile phone, a cordless telephone, a smartphone (combination of a small portable computer and a mobile phone), a PDA (PDA: Personal Digital Assistant) or an organizer. Furthermore the telecommunications devices can also comprise other devices that are accessible by mobile means, such as a personal computer (PC) or a laptop which can be accessed via a mobile radio network by means of a connected mobile radio device (mobile phone). The mobile radio device can then be connected to the personal computer or laptop for example via a cable or also contact said devices wirelessly via an infrared interface or a local Bluetooth network. In this case the first and/or also the further telecommunications devices including the telecommunications network assigned to these can operate in the embodiment of a mobile radio network conforming to the GSM (Global System for Mobile Communication) standard or the UMTS (Universal Mobile Telecommunications System) standard. Such mobile radio networks or telecommunications devices conforming to the GSM or UMTS standard can represent a platform for WAP protocols or the WAP protocol stack (WAP: Wireless Application Protocol) by means of which data (messages and/or user data objects) can be transmitted in the respective mobile radio network. In the case of the use of the WAP protocol stack it is possible, through the use of a WAP gateway as the interface between a mobile radio network and another network, for example a network based on an Internet protocol, to establish a connection to said network. In this way it is possible that the data provisioning component is situated in a network

based on an Internet protocol, such as the Internet, whereby the data (messages, user data objects) can be transmitted via a WAP gateway and finally via an air interface of a mobile radio network between the base station(s) of the mobile radio network and to the respective telecommunications devices.

According to an advantageous embodiment the user data objects can be data in the form of text data, image data or, as the case may be, video data, audio data, executable programs or software components or a combination of these data types, i.e. multimedia data or content.

Preferred embodiments of the present invention will be explained in more detail below with reference to the attached drawings, in which:

Figure 1 is a block diagram showing the components involved in a method for downloading user data objects including the data flow between the components;

Figure 2 is a block diagram showing the components involved in a method for downloading or transmitting rights objects including the data flow between the components;

Figure 3 shows a schematic representation of a container object according to an embodiment of the invention;

Figure 4 shows a schematic representation of a rights object according to an embodiment of the invention;

Figure 5 shows a schematic representation of a confirmation object assigned to the rights object according to an embodiment of the invention.

A method proposed by the WAP Forum or its successor organization OMA (OMA: Open Mobile Alliance) for downloading or transmitting any data objects to telecommunications devices such as mobile radio devices or mobile phones and for managing the rights for the (digital) user data objects essentially consists of two sections, namely the actual downloading or transmission of the user data objects ("content download") and the management of the digital rights ("Digital Rights Management").

As can be seen in Figure 1, a telecommunications arrangement for performing a method for downloading or transmitting user data objects comprises a data provisioning component for providing user data objects and a (first) telecommunications device A. In the example the telecommunications device is embodied as a mobile phone which can operate in accordance with the GSM or UMTS standard. It is further assumed that the mobile phone A is part of a mobile radio network. The mobile phone A is able to use WAP protocols (e.g. Wireless Session Protocol: WSP, etc.) or the WAP protocol stack in order to transmit data over an air interface to a corresponding stationary transmit/receive arrangement of the mobile radio network assigned to the mobile phone A. The data provisioning

component D can be provided in the mobile radio network assigned to the mobile phone A or can be provided for example in the Internet, which is connected to the mobile radio network of the mobile phone A via corresponding WAP gateways. Although it is possible that a user data object can be transmitted from the data provisioning component D to the mobile phone A not only directly, but also via further data provisioning components which together form a data provisioning system, or even can also be transmitted via further mobile phones, the direct transmission of user data objects from the data provisioning component D to the mobile phone A shall be explained in the following description for the sake of simplicity.

As can be seen in the components identified in Figure 1, two logical units are required for a method for transmitting or downloading user data objects, namely firstly a so-called "download server" and secondly a so-called "download client":

1.) The download server HS, which is implemented in particular by means of a software application or a software program on a data provisioning component such as a data server, is responsible on the one hand for providing the download clients on a telecommunications device or a mobile phone firstly with description information relating to a specific object managed by the download server. Description information of this kind is also referred to as meta data or as an object description. Based on a request by a user of a download client on said user's telecommunications device, the download server delivers a desired user data object to said client. In the process the

download server can take into account previously optionally transmitted attributes of the download client or the telecommunications device on which said client is executed or a device connected to the telecommunications device by selecting a user data object matched to the attributes or generating such an object specifically for the download client which is serving as the current recipient.

2.) The download client HK represents in particular a software application on a telecommunications device such as the mobile phone A or an application on a data management device connected to the telecommunications device such as, for example, a portable computer or a PDA. The download client first negotiates the delivery of a desired user data object with the download server, receives said object and confirms its error-free reception to the download server and possibly also the usability of the received content on the telecommunications device or the mobile phone A, as used in the example.

The process for downloading or transmitting user data objects from the download server to the download client, as will be explained further below in relation to Figure 1, is designed so as to fulfill the following requirements:

Before a user downloads a user data object from a data provisioning component he or she must, as already mentioned, first be informed about the attributes of the user data object (for example by means of an object description or description information). Corresponding information can include such things as: the name of the

user data object, the data volume for the transmission of the user data object (e.g. in bytes), a (verbal) description of the user data object, and any further attributes of the user data object to be downloaded.

The user must be able to issue his or her explicit approval (acceptance of the offer by the data provisioning component) for the delivery and possibly the charging of the user data object.

Reference is made once again to Figure 1, in which the process of downloading a user data object is presented in detail, whereby the message flow and action sequence in time is identified by the numbers on the arrows in Figure 1:

1.) The download client HK on the mobile phone A requests description information BI1 from the download server of the data provisioning component D, which contains the object description or meta data relating to a specific user data object.

2.) The description information BI1 is transmitted to the download client HK by the download server HS. Based on the received description information the usability of the described user data object on the mobile phone A of the user can be checked and the approval of the user obtained for downloading the user data object (not shown explicitly here).

3.) The download client HK requests the user data object NDO from the download server HS.

4.) The download server HS sends the chosen user data object to the download client HK.

5.) The download client HK, for its part, sends a status report SR back to the download server HS.

According to a variant already described in the introduction for preventing an unauthorized access to a user data object or an unauthorized use of a downloaded data object, a user data object is encrypted by a data provisioning component of a data provisioning system and provided together with a checksum of the user data object in a container object or a container file. Container objects of this kind can then be transmitted according to the same method as already shown, for example, for unencrypted user data objects in Figure 1.

Starting from a case of this kind, in which an encrypted user data object provided in a container is present on a user's telecommunications device, it is now necessary for the user of the telecommunications device to obtain the rights to use the transmitted container object. According to the embodiment described in the following, such rights can be transmitted by the data provisioning component to the user's telecommunications device by means of a rights object. Such a rights object, which will also be explained later in relation to Figure 4, includes for example a description of the rights which are granted to the user in order to use the encrypted user data object provided in the container object, a reference to the container object which enables an assignment of the rights object to the corresponding container object, and a key with which the encrypted user data object can be decrypted so that it can

subsequently be used. As will be explained further in relation to Figure 2, it is necessary, in order to use the combination of the encrypted user data object, a container object and a rights object, for a special device or software application to be provided on the user's telecommunications device, which device or software application is referred to as a so-called DRM (Digital Rights Management) agent. The DRM agent receives the rights object which has been transmitted by a data provisioning component to the telecommunications device and is responsible for the management of the rights object or, as the case may be, for the safekeeping of its secret, i.e. the key for decrypting the encrypted user data object in the container object. In practice the DRM agent must store the rights object on the telecommunications device and protect it against unauthorized access by other devices or applications. In a method to be explained below in Figure 2, according to an embodiment of the invention in which rights or rights objects are transmitted to a telecommunications device of a user irrespective of user data objects (packed in container objects and encrypted), the following criteria are to be taken into account:

- A check of the integrity or, as the case may be, freedom from damage of a container object or of the encrypted user data object contained in said container object shall be possible even if the container object has been transmitted to the telecommunications device of a user by "superdistribution" and potentially comes from an unreliable source. For this purpose, according to a preferred embodiment of the invention, a checksum of the encrypted user data object is inserted as an additional information element into a description section of the

container object by a data provisioning component (see also Figure 3). In this case the checksum can also be calculated by means of a hash function or a hash algorithm. Here, from a data object of arbitrary size, a hash function can calculate a character string of fixed length (e.g. 128 or 160 bits) with the following attributes. The character string is unique to the data object ("digital fingerprint"). Even changing a single bit of the data object results in a totally different hash value. The original data object cannot be reconstructed from the hash value. It is practically impossible to find two data objects that produce the same hash value. Alternatively the checksum or the hash value can also be calculated over the entire container object. The above-mentioned DRM agent for managing rights of a user data object on a user's telecommunications device can thus check the integrity or freedom from damage of the encrypted user data object only on the basis of the container object by using the defined and generally known algorithm for calculating the checksum or the hash value to calculate precisely this checksum/hash value for the encrypted user data object or the entire container object and comparing it with that in the container object.

- The user shall be able to request new rights or rights objects for an encrypted user data object, packed in a container object, provided on his or her telecommunications device. For this purpose a resource ("rights issuer") can be specified in the container object, or more precisely, in its description section (cf. Figure 3), from which the DRM agent starts to download a rights object, corresponding to the

downloading of user data objects shown in Figure 1. This enables rights or rights objects to be downloaded to the telecommunications device with the reliability corresponding to the "normal" download process for user data objects. To put it more precisely, there can be provided in the description section of the container object a URL (URL: Uniform Resource Locator) which specifies, for example, an "address" of a specific data provisioning component which may be identical to the data provisioning component for user data objects. As a result of the invocation of the specified URL by one of the applications, download client or DRM agent, a user can be provided (via a menu structure, for example) with an offer of one or more different rights, whereby the user can have delivered to him or her by means of a download process or can purchase a specific right or specific rights in the form of rights objects. The user is thus offered a familiar interface and manner of operation such as he or she already knows from the downloading of user data objects to his or her telecommunications device, which increases the confidence in the service.

- In order to guarantee that a specific selected rights object (which is located on a data provisioning component) matches a container object residing on the telecommunications device of a user or the encrypted user data object packed therein, and in order therefore to prevent an incorrect rights object, for which he or she must still pay, being transmitted to a user of a telecommunications device, a confirmation object ("verifier object") assigned to the rights object is to be transmitted first to the telecommunications device of

the user instead of the rights object. This confirmation object contains the checksum or hash value of the encrypted object, packed in a container object, that is already present on the telecommunications device of the user or the checksum (the hash value) of the container object. The confirmation object can further contain an identification designation for the container object to be checked so that the DRM agent responsible for rights management is able to check the right container object is stored on the telecommunications device of the user. This means that a new object type, namely that of the confirmation object is defined, by means of which DRM-relevant data can be transmitted from the download server of a data provisioning component to the DRM agent of a telecommunications device without the need to transmit the actual rights object itself. By this means a separation of DRM-relevant data and content-related data and an implementation of an essentially identical execution of the download process for additional rights or rights objects are created with an additional guarantee of the relatedness of the encrypted user data object already present on the telecommunications device of a user and the rights object to be downloaded.

- According to a possible embodiment of the explained variant, already prior to or during the request for new rights or rights objects the DRM agent checks the checksum or hash value relating to the container object or encrypted user data object packed therein for correctness and/or integrity. This reduces the overhead for checking the checksum or hash value following reception of the confirmation object to a comparison between the just checked or, as the case may be, newly

determined checksum (or hash value) and the checksum (or hash value) provided in the confirmation object. In this way the time period for sending a status report to the download server on completion of the comparison or the time for requesting the actual rights object can then be reduced.

- If the check of the checksum (or hash value) transmitted by the confirmation object is negative, i.e. if the checksum provided in the confirmation object does not tally with the checksum, newly determined by the DRM agent, of the encrypted user data object or the entire container object, the process of downloading the actual rights object can be interrupted, as a result of which the user of the telecommunications device who wanted to download a rights object is protected from downloading a rights object that he or she cannot use, and so is protected from having to pay for said unusable rights object.

A process flow scheme for illustrating the method for transmitting or downloading rights or a rights object will now be described below with reference to Figure 2, whereby the data flow in time and method sequence are identified by means of the numbers 1 to 9 on the arrows in Figure 2. In this case it is assumed that there is already provided on the telecommunications device of a user to which a rights object is to be transmitted an encrypted user data object, packed in a container object, in a memory area of the telecommunications device, which user data object comes, for example, from a data provisioning component by means of a method, illustrated in Figure 1, for downloading user data objects or has been transferred by another

telecommunications device. It is further assumed in Figure 2 that the download server HS according to Figure 1 is an application on a data provisioning component D of a data provisioning system, while the download client HK and the DRM agent DRMA are applications or software applications on a user's telecommunications device or, as the case may be, mobile phone A to which a specific rights object is to be transmitted.

1.) A resource of the rights provider (data provisioning component D) is requested or invoked by the DRM agent DRMA using the corresponding URL which is specified in the description section of the corresponding container object on the mobile phone A of the user in order to download or transmit a rights object RO. This causes a new download process to start. The purpose of the request is to receive description information which is transmitted to the mobile phone A and evaluated there accordingly by the download client HK and responded to. Alternatively a browsing session can also take place between the calling of the resource by the DRM agent and the transmission of the description information BI1, i.e. the immediate response to the initial request or inquiry in the agent DRMA includes, not description information, but one or more web pages which describe, for example, an offer for downloading new rights and contain a reference for downloading the description information. However, at the end of the browsing session, following selection of a specific rights object, description information is again requested by the mobile phone A or the DRM agent.

2.) The description information BI1 is transmitted to the mobile phone A and passed according to its type to the download client HK. In this case the transmission of the description information from the data provisioning component D to the mobile phone A can take the form, for example, of a message in the Short Message Service (SMS), a message in the Multimedia Message Service (MMS), an e-mail or an instant message, etc.

3.) The download client HK presents the information for the user for example on a display of the mobile phone A and checks whether the content type or types listed in the description information BI1 can be used by the mobile phone A. This means that a check is made to determine whether the mobile phone A is able to display or play back certain content, such as image data at a particular resolution or color or also music data. If this is the case and the user gives his or her approval, the download client HK requests the transmission of the confirmation object DCFV, to which in this example the request for the actual rights object RO is logically linked.

4.) As a response to the request, the download server transmits the confirmation object DCFV to the download client HK.

5.) The download client HK recognizes the type of the confirmation object DCFV, has stored an assignment to the DRM agent DRMA for said object or file type and passes the confirmation object to the DRM agent for checking.

6.) The DRM agent checks whether the checksum (or hash value) contained in the confirmation object DCFV tallies with the checksum (or hash value) of the container object DCF already stored on the mobile phone A. For this purpose the confirmation object DCFV also contains the identification designation of the container object DCF. The DRM agent DRMA has stored information associated with this identification designation indicating where in the memory of the mobile phone A the corresponding container object is stored, which value the checksum (or hash value) of the container object or the encrypted user data object packed therein has, and whether the check or comparison of the checksum (or hash value) has been completed successfully.

7.) If the matching container object has been found in step 6.) and the checksum (or hash value) has been checked successfully, i.e. if the checksum contained in the confirmation object tallies with the checksum of the container object stored on the mobile phone A or the encrypted user data object contained therein, the DRM agent DRMA issues a positive message to the download client HK.

8.) The download client HK sends a status report to the download server HS in which the result obtained in step 7.) is passed on.

9.) Upon receiving a positive status report the download server transmits the requested rights with the actual rights object RO in, for example, a "push" mode (e.g. by means of a WAP push) to the mobile phone A. It is

entirely possible that a transmission of said kind can also be performed by means of a message in the MMS or as an e-mail. The DRM agent DRMA now receives the rights object RO and stores it in a special memory area which is protected against unauthorized access. Using the key contained in the rights object RO the DRM agent DRMA can decrypt the encrypted user data object contained in the container object DCF and finally make it usable for use by the user of the mobile phone. For example, image data contained in the user data object can be displayed on a display device of the mobile phone, music data can be audibly played back or multimedia data such as video clips can also be displayed and played back, etc.

Following the above explanation of a general example for transmitting or downloading rights or rights objects from a data provisioning component to a telecommunications device such as a videophone, a more concrete example will now be explained.

Let it be assumed as the starting situation that on the mobile phone (A) there is stored a container object which has reached the mobile phone (A) by means of superdistribution (i.e. a transmission from a further mobile phone). For example, the container object DCF was transferred to the mobile phone (A) as part of a multimedia message in the Multimedia Messaging Service (MMS) or simply via an infrared interface (IrDA). It is then stored in a memory area provided for data objects or in a file system of the mobile phone (A) and can be identified there as a container object by a special file extension. If the user of the mobile phone (A) activates the container object (for

example by selecting it in a file management application such as an Explorer), the DRM agent is started automatically in order to search for a matching rights object for the selected container object. It is assumed that no rights object has yet been transferred to the mobile phone (A) for the container object, with the result that the DRM agent (DRMA) is not successful in its search for a suitable rights object and proposes to the user to obtain rights or a rights object off the Internet from the associated rights provider and download it to the mobile phone (A). For this purpose a description section in the container object contains an Internet address or URL of the rights provider. Also stored in the description section of the container object (see also Figure 3) in addition to the URL of the rights provider is the checksum (or hash value) of the encrypted user data object packed in the container object, by means of which the integrity or freedom from damage of the container object and hence of the packed, encrypted user data object can be checked. If the user selects the URL for downloading new rights for the encrypted user data object, on the one hand the referenced URL is selected and on the other the checksum (or hash value) for the encrypted user data object packed in the container object is determined by the DRM agent in order to verify its integrity. The result of this integrity check is stored by the DRM agent, as also is the identification designation for the container object and its position in the file system on the mobile phone (A).

The invocation of the resource (data provisioning component of a rights provider) at the address specified in the description section of the container object ("rights issuer URL") has a result that depends on the embodiment by the

rights provider. Either a web page is returned (e.g. in the HTML (Hypertext Markup Language) format or in another, for example an XML-based, format), a browser application is started on the mobile phone A and a browsing session follows in which the user of the mobile phone (A) is offered an address for starting the download process for new rights. As an alternative to the return of a web page and a following browsing session the download process can be started directly by retrieval of description information for a specific container object or the user data object contained therein.

The encrypted user data object matching the requested rights can be described in the description information processed by the download client (HK) of the mobile phone (A) just as accurately as if the encrypted user data object itself were to be downloaded. Thus, when downloading new rights, the user of the mobile phone (A) receives the same information as when downloading the encrypted user data object and thus has the same basis on which to make a decision whether to make use of the proposed service (rights) or not. In contrast to the download process for the encrypted user data object and the associated rights object, however, the type of a confirmation object assigned to the rights object is specified in the description information as content type for the download process. By this means the download client and also the user are informed that only the rights object or a confirmation object assigned thereto will be transmitted. The corresponding encrypted user data object must therefore already be stored on the mobile phone (A). In addition, the download client can check on the basis of the other specifications in the description information that relate

to the encrypted user data object whether the described encrypted user data object or its content can also be used on the mobile phone (A), i.e. whether attributes such as size, type and further attributes of the unencrypted user data object "match" the device features of the mobile phone (A).

If all the above-mentioned criteria are met and the user decides to download new rights, the download client continues the download process by requesting the confirmation object assigned to the rights object from the download server (HS). The download server responds and sends the confirmation object to the download client, which recognizes the object type of the confirmation object and immediately passes on the confirmation object to the DRM agent. The DRM agent receives the confirmation object, interprets the identification designation for the relevant container object contained therein in order to determine which (container) object needs to be checked and compares the checksum (or hash value) received in the confirmation object with the corresponding value contained in the description section of the container object or with the previously determined value of the encrypted user data object in the container object. If the checksums (or hash values) tally, it is confirmed that the encrypted user data object in the container object will be usable with the previously selected rights object. The DRM agent then signals a positive check of the confirmation object to the download client. The download client thereupon sends the download server a status report in which the corresponding status value or status report causes the download server to send the previously selected rights object, for example by means of a WAP push, to the mobile phone (A) and possibly

to charge the user for the associated service (i.e. the use of the user data object in the container object). This can be accomplished by the sending, by the download server, of an instruction to a billing system of the mobile radio network in which the mobile phone (A) resides to charge the user of the mobile phone (A) for the downloaded rights or rights object, for example using the traditional telecommunications call billing system.

Following the arrival of the rights objects on the mobile phone (A), said rights object is passed on in turn according to its object type immediately to the DRM agent and managed by the latter. The object can be located and opened in the memory of the mobile phone (A) via a management data record or an identification designation of the container object. Next, the key contained in the (new) rights object is used for decrypting the encrypted user data object in the container object and the user data object can then be used.

Reference will now be made to Figure 3, which shows a container object DCF which can be used for example in a method illustrated in Figure 2. The container object DCF comprises a content section IA, in which an encrypted user data object vNDO is stored, and a description section BA, in which there are provided an identification designation "Content ID" for the container object DCF, a rights provider URL, which can be used for requesting new rights, and a checksum (or hash value) by means of which the integrity or freedom from damage of the encrypted user data object or the entire container object can be checked.

Reference will now be made to Figure 4, which shows a rights object RO which can be used for example in the method illustrated in Figure 2. In a general description section ABA, the rights object RO contains, in addition to other possible identifiers or elements, an identification designation "Content ID", which serves to identify the associated container object DCF. The rights object RO also contains a rights description section RBA, which contains a key for decrypting the encrypted user data object vNDO contained in the container object DCF and also a description of the rights for usage of the encrypted user data object vNDO. The description of the rights includes, as already mentioned above, the definition of the rights which the user receives by way of the transferred rights object in order to use the encrypted user data object, specifying, for example, that the user may only listen to music data even if image or video information is also contained in the encrypted user data object. However, the user can also receive the rights for full use of the encrypted user data object, etc.

Reference will now be made to Figure 5, which shows a confirmation object DCFV assigned to the rights object RO depicted in Figure 4. Important elements of the confirmation object DCFV are firstly the identification designation "Content ID" for referencing the associated container object DCF, as has been explained for example in relation to Figure 2, and secondly the checksum (or hash value) which has to be compared with the corresponding value of the container object DCF in order to guarantee correct assignment of a rights object RO that is to be newly downloaded and a container object DCF already present on a telecommunications device of a user.

It should be noted in conclusion that although in the illustrated embodiments of a method for downloading rights objects it has always been assumed that while a container object with an encrypted user data object contained therein is already stored on the telecommunications device, there is not yet an associated rights object present to enable the encrypted user data object to be used. It is, however, also possible that in addition to the container object with the encrypted user data object contained therein, a first rights object is already stored on the telecommunications device of the user, which first rights object thus enables the use of the encrypted user data object based on the rights described therein. However, if these rights of the first rights object permit a partial use of the encrypted user data object, then it is also possible that the user of the telecommunications device would like to download or transmit a second rights object to his or her telecommunications device which allows more extensive or full use of the encrypted user data object. In such a case the user can request the second rights object, as described for example in general terms in relation to Figure 2, and after checking by a confirmation object assigned to the second rights object, download the second rights object to his or her telecommunications device in order to enable more extensive use of the encrypted user data object on his or her telecommunications device ("rights refresh").